UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/821,565	03/29/2001	Mark M. Ishikawa	60123.803US01	5876

34313 7590 02/28/2006

ORRICK, HERRINGTON & SUTCLIFFE, LLP
IP PROSECUTION DEPARTMENT
4 PARK PLAZA
SUITE 1600
IRVINE, CA 92614-2558

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 02/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/821,565	ISHIKAWA, MARK M.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12/19/2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *40-78* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *40-78* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on December 19, 2005. Claims 1-39 have been canceled. Claims 40-78 have been added. Claims 40-78 are pending.

Response to Arguments

2. Applicant's arguments for the newly added claims filed 12/15, 2005 have been fully considered but they are not persuasive. Applicant contends that the cited prior art does not teach or suggest "*rendering a protected network device unreachable to an offending network device and thereby inhibiting the offending network device from clogging an intermediate switching system with problematic information packets as recited in new claims 40-78*" (remark, page 15, last paragraph); Examiner respectfully disagrees. Shanklin clearly teaches routing or switching system with load balancer and intrusion detection sensor and network analyzer to detect certain types of composite signatures to protect the packet from forwarding to protected network and the packet load balancer is especially beneficial under flooding condition (see Fig. 1-6 and col. 4, line 44-col. 5, line 67). Applicant further contends that "*upon detection of problematic information packets, a protected network device is rendered unreachable such that a suspect network device is prevented from transmitting the problematic information packets to an intermediate switching system*" ; "*Shanklin et al., for example, discloses ...the sensor analyzes the data packets to determine whether traffic into and out from the local network is misused and upon detecting an intrusion, "can take appropriate*

action, such as terminating the connection...the system disclosed by Shanklin et al. therefore is wholly incapable of preventing the connection from being subsequently re-established and does nothing to inhibit the intermediate router from becoming clogged due to further intrusions (remark, page 16, 2nd and 3rd paragraph). Examiner agrees that even though Shanklin does not provide detail of what appropriate action encompasses when detection of intrusion is detected, instead, Shanklin disclose one of the actions is terminating the connection. However, Examiner asserts that even if Shanklin's system teaches one of the appropriate action is terminating the connection would still meet the claimed limitation of inhibiting or rendering the second networks unreachable and prevents the first network device from transmitting the problematic information packets to said switching system as claimed in independent claims. Applicant's remark states that Shanklin system is wholly incapable of preventing the connection from being subsequently re-established and does nothing to inhibit the intermediate router from becoming clogged due to further intrusions. First of all, the independent claims does not recite the connection subsequently re-established and even if it were cited, Shanklin's one of appropriate action such as terminating the connection should not be construed to be interpreted as incapable of *subsequently* re-established connection. Secondly, by the meaning of the phrase, terminating the connection, incoming packets will be stopped and consequently the switch or router will be prevented from becoming clogged due to further intrusion.

Claim Objections

3. Claim 52 is objected to because of the following informalities:

The claim is dependent on itself. Examiner assumes the claim intended to read "the system of claim 51. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 56 recites the limitation "said arbitration system" in lines 7. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 40-44, 46-48, 54-56, 59, 60-63, 69-71, 77 and 78 are rejected under 35 U.S.C. 102(e) as being anticipated by Shanklin et al. (U.S. Patent No. 6,578,147, hereinafter Shanklin).

In respect to claim 40, Shanklin discloses system for identifying and diverting problematic information packets transmitted from a first network device to a second

network device, comprising: a switching system that provides a network address of the second network device to the first network device, said switching system receiving the information packets from the first network device and directing the information packets to the second network device (see Fig. 4-6 and col. 7, lines 20-64); a route arbitration system that monitors the information packets received by said switching system, said route arbitration system determining whether the information packets comprise abnormal network activity in accordance with a first predetermined criteria and, if said route arbitration system determines that the information packets comprise abnormal network activity, identifying the information packets as being abnormal information packets; and a traffic analysis system that monitors the abnormal information packets identified by said route arbitration system, said traffic analysis system determining whether the abnormal information packets are problematic in accordance with a second predetermined criteria and, if said traffic analysis system determines that the abnormal information packets are problematic, identifying the abnormal information packets as being the problematic information packets and inhibiting said switching system from providing the network address of the second network device to the first network device, wherein said switching system, when inhibited, renders the second network device unreachable and prevents the first network device from transmitting the problematic information packets to said switching system (see Fig. 4-6, col. 3, lines 60-65, col. 7, lines 20-30).

In respect to claim 41, Shanklin discloses the system of claim 40, wherein said switching system includes a routing system (see Fig. 3 and 4, col. 5, lines 55-61 and col. 7, lines 20-28).

In respect to claim 42, Shanklin discloses the system of claim 40, wherein said route arbitration system is at least partially incorporated into said switching system (see Fig. 3 and 4, col. 5, lines 55-61 and col. 7, lines 20-28).

In respect to claim 43, Shanklin discloses the system of claim 40, wherein said route arbitration system communicates with said switching system via at least one communication link selected from the group consisting of a remote monitoring network probe, a switching device, and an Ethernet probe (see Fig. 3 and 4, col. 5, lines 55-61 and col. 7, lines 20-28).

In respect to claim 44, Shanklin discloses the system of claim 40, wherein said route arbitration system monitors a volume of the information packets (see Fig. 3 and 4, col. 5, lines 55-61 and col. 7, lines 20-28).

In respect to claim 47, Shanklin discloses the system of claim 40, wherein said traffic analysis system is at least partially incorporated into said switching system (see Fig. 3 and 4, col. 5, lines 55-61 and col. 7, lines 20-28).

In respect to claim 48, Shanklin discloses the system of claim 40, wherein said traffic analysis system monitors a volume of the abnormal information packets (see col. 4, lines 39-41).

In respect to claim 54, Shanklin discloses the system of claim 40, further comprising a firewall system that identifies suspect information packets received from the first network device, said switching system directing the information packets to the second network device via said firewall system (see Fig. 2, col. 1, lines 19-16, col. 3, lines 10-18 and col. 5, lines 14-55).

In respect to claim 55, Shanklin discloses the system of claim 54, wherein said traffic analysis system determines whether the suspect information packets are problematic and, if said traffic analysis system determines that the suspect information packets are problematic, inhibits said switching system from providing the network address of the second network device to the first network device (see col. 3, lines 60-65).

In respect to claims 56, 59, 60, 71, 77 and 78, the claimed limitations are similar to claim 1. Therefore, claims 56, 59, 60, 71, 77 and 78 are also rejected for the similar rationale.

In response to claim 61, Shanklin discloses the system of claim 60, wherein said protected network device comprises at least one network device selected from the group consisting of a server system, a computer system, a provider computer system, a user computer system, a router system, an edge router system, a core router system, and a firewall (see Fig. 2, col. 5, lines 14-20).

In response to claim 62, Shanklin discloses the system of claim 60, further comprising a communication system, said switching system communicating with the external network device via said communication system (see Fig. 4, col. 7, lines 20-39).

In response to claim 63, Shanklin discloses the system of claim 62, wherein said communication system comprises a communication link selected from the group consisting of a local area network, a wired communication network, a wireless communication network, a wide area network, a public communication network, and the Internet (see Fig. 2, col. 5, lines 14-20).

In respect to claim 69, the claimed limitation is similar to claim 54. Therefore, claim 69 is rejected based on the similar rationale.

In respect to claim 70, Shanklin discloses the system of claim 60, wherein said traffic analysis system instructs said switching system to redirect the information

packets to a traffic analysis device, said traffic analysis device receiving and analyzing the information packets (see col. 5, lines 14-55).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 46, 65 and 74 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin (U.S. patent No. 6,578,147) in view of Schuba (U.S. Patent No. 6,725,378).

In respect to claim 46, Shanklin discloses the system of claim 40. Shanklin does not explicitly discloses wherein said route arbitration system, upon determining that the information packets no longer comprise said abnormal network activity, enables said switching system to again provide the network address of the second network device to the first network device and receive the information packets from the first network device. However, Schuba discloses data packets are classified to be in different states and depending on the changes of the state of the addresses, closing or open the corresponding connection based on the observed behavior of the network traffic (see col. 11, lines 1-26). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching Shanklin's detection system

with Schuba's opening or closing of the connection depending on the change of address state for the benefit of determining the opening or closing of the network connection based on the observed behavior of the network traffic (see col. 11, lines 23-26).

In respect to claims 65 and 74, the claimed limitation is similar to claim 46. Therefore, claims 65 and 74 are rejected based on the similar rationale.

7. Claims 45, 49, 50, 57, 58, 64, 66, 67, 72 and 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin (U.S. Patent No. 6,578,147) in view Putzolu et al. (U.S. Patent No. 6,587,432).

In respect to claims 49 and 50, Shanklin discloses the system of claim 48, wherein said traffic analysis system determines that the abnormal information packets are problematic (see col. 4, lines 39-41) but does not explicitly discloses when the volume of the abnormal information packets is greater than a preselected volume threshold level or when the volume of the abnormal information packets does not decrease during a preselected time interval. However, Putzolu discloses a network monitoring agent and a tracing agent monitors and analyze traffic on a network to detect network congestion condition (see col. 1, lines 41-55 and col. 3, line 43-col. 4, line 4, "congestion traffic may be traffic which existed prior to a excess traffic condition, such as in the case where other additional traffic, when added to a network, causes an excess traffic condition...or may be the traffic which existed on the healthy link prior to the failure..." (Putzolu, col. 1, lines 42-49). It is inherently required that a predetermined

parameter is needed in order to determine whether the traffic volumes have reached a congestion condition). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the traffic monitoring and analyzing of network traffic volume to detect network congestion condition taught by Putzolu with the intrusion detection for identifying and detecting network attack with stored signature such as denial of service so that information about congestion traffic can be quickly and accurately collected (Putzolu, col. 2, lines 51-56).

In response to claims 57, 58, 64, 66, 67, 72 and 73, the claimed limitations are similar to claims 45 and 50. Therefore, claims 57, 58, 64, 66, 67, 72 and 73 are rejected based on the similar rationale.

8. Claims 51, 52, 53, 75 and 76 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shanklin (U.S. patent No. 6,578,147) in view of Gibbings (U.S. Patent No. 6,885,675).

In respect to claims 51 and 52, Shanklin discloses the system of claim 40. Shanklin does not disclose a null network device having a null address, said null network device receiving the information packets and providing no response to the first network device such that the first network device transmits the problematic information packets to said null network device. However, Gibbings discloses a null router used to route data packet to null (see col. 5, lines 3-19). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the teaching of

Shanklin's detection system with Gibbings' teaching of routing data packet to null in order to prevent large amount of data floating into a particular downstream router (see col. 5, lines 9-15).

In respect to claim 53, Shanklin and Gibbings disclose the system of claim 52, wherein said null network device is provided by at least one of said route arbitration system and said traffic analysis system (see col. 5, lines 9-15).

In respect to claims 75 and 76, the claimed limitations are similar to claims 51. Therefore, claims 75 and 76 are rejected based on the similar rationale.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

February 17, 2006

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER